UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/036,521	01/07/2002	Robert John Ackroyd	01.119.01	5107

7590 12/20/2006

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/20/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/036,521	**Applicant(s)** ACKROYD, ROBERT JOHN	
	Examiner Eleni A. Shiferaw	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Pre-Appeal conference has been held on December 14, 2006 with Lee, Eddie and Moazzami, Nasser. In view of the conference the examiner hereby reopens the Office action.

Response to Arguments

2. Applicant's arguments with respect to claims 1-29 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. Claims 1-4, 6-13, 15-22, and 24-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schertz et al. (Schertz, Pub. No.: US 2003/0084322 A1) in view of Brook et al. USPN 7,036,148 B2.

As per claims 1, 10, and 19, Schertz teaches a computer program product/method/apparatus for controlling a managing computer to manage malware protection within a computer network containing a plurality of network connected computers, said computer program product comprising:

receiving code operable to receive at said managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers (page 4 par. 0030 lines 9-10, and page 3 par. 0022 lines 8-10);

detecting code operable to detect from said plurality of log data messages received by said managing computer a pattern and **a network-wide (par. 0021, 0023, 0018, 0003, and par. 0018 of Schertz discloses:** ***virus intrusion detecting/monitoring/scanning of ALL devices on a network network-wide, network-based virus intrusion detection system typically monitors all network activity and network traffic, Network-based virus intrusion protection systems analyze data inbound from the internet and collects network packets to compare against a database of various known attack signatures or bit patterns***) of malware detection across said plurality of network connected computers matching one or more predetermined trigger (page 4 par. 0030 lines 9-21, page 3 par. 0021 lines 10-18, and par. 0023 lines 12-18); and

action performing code operable in response to detection of one or more predetermined trigger patterns to perform one or more predetermined anti-malware actions (page 4 par. 0030 lines 16-21, and page 3 par. 0020 lines 14-25).

Schertz fails to disclose a threshold malware detection; and

the network-wide threshold being applied to a sum of detections each being associated with a different one of the network connected computers.

However Brook et al. discloses threshold malware detection in a network-wide across said plurality of network connected computers matching one or more predetermined trigger (see col. 2 lines 21-55, col. 4 lines 7-col. 5 lines 36, and col. 3 lines 12-30); and

the network-wide threshold being applied to a sum of detections each being associated with a different one of the network connected computers (col. 3 lines 12-30, and col. 4 lines 7-col. 5 lines 57).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Brook et al. within the system of Schertz because they are analogous in intrusion detection. One would have been motivated to incorporate the teachings of Brook et al. because it would provide an efficient detection of intrusion by setting rules like frequency-of-occurrence stipulations, and count-reset instructions associated with a signature.

As per claims 2, 11, and 20, Schertz further teaches a computer program product/method/apparatus, wherein said plurality of network connected computers each have a malware scanner that serves to scan computer files to detected malware within said computer files (page 4 par. 0031 lines 1-3).

As per claims 3, 12, and 21, Schertz teaches a computer program product/method/apparatus, wherein said malware scanner uses malware definition data to identify malware to be detected (page 4 par. 0031 lines 1-3, and fig. 1 No. 16).

As per claims 4, 13, and 22, Brook et al. further teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include forcing an update of malware definition data being used by one or more of said plurality of network connected computers (fig. 5 and col. 5 lines 59-col. 6 lines 34). It would have been obvious to combine the teachings of Brook within the system of Schertz because it would keep the detection device current.

As per claims 6, 15, and 24, Schertz teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include isolating one of more of said network connected computers from other parts of said computer network (page 4 par. 0031 lines 17-24 and page 3 par. 0020 lines 14-17).

As per claims 7, 16, and 25, Schertz teaches a computer program product/method/apparatus, wherein said managing computer stores said plurality of log data messages within a database (fig. 2 No. 80A and 81A and par. 0021 lines 15-18).

As per claims 8, 17, and 26, Schertz teaches a computer program product/method/apparatus, wherein said detecting code is operable to query said database (page 18 lines 7-10).

As per claims 9, 18, and 27, Schertz teaches a computer program product/method/apparatus, wherein said database includes data identifying one or more of:

malware protection mechanisms used by respective network connected computers (page 2 par. 0016 lines 14-17);

versions of malware protection computer programs used by respective network connected computers (page 4 par. 0031 lines 1-3, and fig. 1 No. 16);

versions of malware definition data used by respective network connected computers (page 4 par. 0031 lines 1-3, and fig. 1 No. 16); and security settings of malware protection mechanisms used by respective network connected computers (page 2 par. 0016 lines 14-17).

As per claim 28, Schertz discloses a program stored on a computer-readable medium as claimed in claim 1, wherein predefined network-wide thresholds and patterns are provided as templates (0021 lines 15-18; *network-wide patterns are provided as a template*).

As per claim 29, Schertz discloses a program stored on a computer-readable medium as claimed in claim 1, wherein predefined network-wide thresholds and patters are customized to particular circumstances (0021; *customized to ... detecting, comparing circumstances...)*

4. Claims 5, 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schertz et al. (Schertz, Pub. No.: US 2003/0084322 A1) and Brook et al. USPN 7,036,148 B2 in view of Chen et al. (Chen, Patent Number: 5,832,208).

As per claims 5, 14, and 23, Schertz teaches all the subject matter as described above.
Schertz does not explicitly teach altering the scanner setting when malware is detected.
However Chen teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning (Chen Fig. 3 No. 260; performing more thorough virus scanning after virus is detected).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Chen within the combination system of Schertz and Brook et al. because it would scan the entire email/data to detect more virus if any.

5. Claims 1-4, 6-13, 15-22, and 24-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Chefalas et al. US PG PUBS 2002/0116639 A1.

As per claims 1, 10, and 19, Chefalas teaches a computer program product/method/apparatus for controlling a managing computer to manage malware protection within a computer network containing a plurality of network connected computers (**fig. 1 and claim 29**), said computer program product comprising:

receiving code operable to receive at said managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers (**0027, and 0057-0058; identified malware detections are received at the *server 106 from plurality of client devices over the networks***);

detecting code operable to detect from said plurality of log data messages received (***0012, fig. 4A-B, and fig. 5A-B; detecting at users computers and received at the server***) by said managing computer a pattern and a network-wide of malware detection across said plurality of network connected computers matching one or more predetermined trigger, (***0012, fig. 4A-B, and fig. 5A-B; multiple patterns are detected and transmitted to the server network-wide threshold)*** the detections each being associated with a different one of the network connected computers (fig. 1 and 0022); and action performing code operable in response to detection of one or more predetermined trigger patterns **to perform one or more predetermined anti-malware actions (0012 and fig. 8 element 804).**

Chefalas et al. fails to disclose threshold of malware detection; and

the threshold being applied to sum of detections.

However Brook et al. discloses a threshold of malware detection across said plurality of network connected computers matching one or more predetermined trigger (see col. 2 lines 21-55, and col. 3 lines 12-30, and col. 4 lines 7-col. 5 lines 36); and

the threshold being applied to sum of detections, the detections each being associated with a different one of the network connected computers (col. 3 lines 12-30, and col. 4 lines 7-col. 5 lines 57).

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Brook et al. within the system of Chefalas et al. because they are analogous in intrusion detection. One would have been motivated to incorporate the teachings of Brook et al. because it would provide an efficient detection of intrusion by setting rules like frequency-of-occurrence stipulations, and count-reset instructions associated with a signature.

As per claims 2, 11, and 20, Chefalas et al. further teaches a computer program product/method/apparatus, wherein said plurality of network connected computers each have a malware scanner that serves to scan computer files to detected malware within said computer files (fig. 1 elements 128, 132, 134, and 136).

As per claims 3, 12, and 21, Chefalas et al. teaches a computer program product/method/apparatus, wherein said malware scanner uses malware definition data to identify malware to be detected (fig. 4A, and Fig. 5A; *virus names A-F*).

As per claims 4, 13, and 22, Brook et al. further teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include forcing an update of malware definition data being used by one or more of said plurality of network connected computers (fig. 5 and col. 5 lines 59-col. 6 lines 34). It would have been obvious to combine the teachings of Brook within the system of Chefalas et al. because it would keep the detection device current.

As per claims 6, 15, and 24, Chefalas et al. teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include isolating one of more of said network connected computers from other parts of said computer network (fig. 6 element 606 and fig. 7 element 706).

As per claims 7, 16, and 25, Chefalas et al. teaches a computer program product/method/apparatus, wherein said managing computer stores said plurality of log data messages within a database (fig. 5A).

As per claims 8, 17, and 26, Chefalas et al. teaches a computer program product/method/apparatus, wherein said detecting code is operable to query said database (0048).

As per claims 9, 18, and 27, Chefalas et al. teaches a computer program product/method/apparatus, wherein said database includes data identifying one or more of:

malware protection mechanisms used by respective network connected computers (0048);

versions of malware protection computer programs used by respective network connected computers (fig. 5A);

versions of malware definition data used by respective network connected computers (fig. 5A); and

security settings of malware protection mechanisms used by respective network connected computers (fig. 8 element 804, and 0012).

As per claim 28, Brook et al. discloses a program stored on a computer-readable medium as claimed in claim 1, wherein predefined network-wide thresholds and patterns are provided as templates (fig. 3 elements 301B-304B and 301D-304D). It would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Brook et al. within the combination system because it would detect intrusion based on known signature and threshold values /rules so it would enhance the detection system.

As per claim 29, Brook et al. discloses a program stored on a computer-readable medium as claimed in claim 1, wherein predefined network-wide thresholds and patters are customized to particular circumstances (col. 4 lines 7-col. 5 lines 58). The rational for combining are the same as claim 28 above.

6. Claims 5, 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chefalas et al. US PG PUBS 2002/0116639 A1, and Brook et al. USPN 7,036,148 B2, and in view of Chen et al. (Chen, Patent Number: 5,832,208).

As per claims 5, 14, and 23, Chefalas et al. teaches all the subject matter as described above. Chefalas does not explicitly teach altering the scanner setting when malware is detected. However Chen teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning (Chen Fig. 3 No. 260; performing more thorough virus scanning after virus is detected). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Chen within the combination system of Chefalas and Brook et al. because it would scan the entire email/data to detect more virus if any.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 2004/0230840 A1 Radatti: discloses *viruses, Trojan, horses, worms, and etc...*

detection over a network. Receiving and detecting all data streams that pass from an external network, through the transport layer of an operating system to the user application or fro the user application to the transport layer.

US 2004/0088570 A1 Roberts et al. *discloses internet data malware scanning.*

US 2003/0177397 A1 Samman *discloses network environment virus detection and protection.*

US 2003/0023866 A1 Hinchliffe et al. *discloses centrally managed malware scanning and detecting method.*

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 18, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/18/06